Computing Policy

including the Acceptable Usage of ICT Equipment

St Agnes C of E Primary School

Approved by:	Sue Gittins
Last reviewed on:	September 2026
Next review due by:	September 2027

Computing Policy
including the Acceptable Usage of ICT Equipment

Our Christian Vision

'Learning together in God's Love'

Our Christian Vision

St Agnes is an inclusive Christian family, we want our children to:

- Learn together with respect, patience and kindness
- **Treat each other as they would like to be treated (Matthew 7v12)**
- Flourish in education and friendships
- **Live life in all its fullness (John 10v10)**
- Be proud of themselves and others
- Ensure everyone is treated equally

Through the range of experiences we offer to all our pupils we encourage an understanding of the meaning and importance of faith and promote all the Christian Values. We particularly focus on Responsibility, Creativity, Forgiveness, Perseverance, Hope, Thankfulness and Friendship. These Christian values form the basis of our vision and are embedded throughout our school life and underpin all our teaching.

St Agnes is a small school that supports our community by providing an education of the highest quality within the context of Christian belief and practice. We work closely with our families to ensure they are fully supported and cared for.
We expect everyone at St Agnes C of E Voluntary Aided Primary School to follow 'The Great

Expectations' –

Be Safe
Be in the right place at the right time
Do your best
Handle your emotions
Use appropriate language
Cooperate
Respect everyone and everything

1. Introduction

Computing is integral to the curriculum at St Agnes C of E Primary School. We aim to equip children with the knowledge, skills and judgement needed to use digital technology confidently, creatively, safely and responsibly. This policy sets out our approach to computing teaching and the acceptable use of school digital technology. It should be read alongside the school Online Safety Policy, Artificial Intelligence Policy, Filtering and Monitoring Policy, Data Protection Policy, Safeguarding/Child Protection Policy and Staff Code of Conduct. From September 2026, this policy reflects Keeping Children Safe in Education 2026, the Department for Education (DfE) digital and technology standards (including the filtering and monitoring and cyber security core standards), the statutory Mobile phones in schools guidance, and the UKCIS Education for a Connected World framework.

2. Aims and Objectives

The aims of our Computing Policy are to:

- **Develop Digital Literacy:** Enable pupils to confidently find, evaluate, and use digital information across various platforms. This includes understanding how to critically assess the validity of information found online.
- **Enhance Creative Expression:** Encourage pupils to use technology creatively for various purposes such as digital storytelling, graphic design, and multimedia presentations.
- **Promote Problem-Solving Skills:** Teach computational thinking through activities that require pupils to break down complex problems, develop algorithms, and implement solutions using code.
- **Ensure Safe Internet Use:** Educate pupils about the risks of the internet, including cyberbullying, privacy concerns, and exposure to inappropriate content, and empower them to use the internet safely and responsibly.
- **Foster Collaboration and Communication**: Use digital tools to facilitate collaborative projects and effective communication among pupils both locally and globally.
- **Support Curriculum Integration:** Integrate computing skills across the curriculum, enhancing learning in subjects such as mathematics, science, and the humanities.
- **Embed Online Safety Across Subjects:** Integrate online safety into all subject areas, teaching pupils how to be safe and responsible digital citizens across various contexts.
- **Promote Digital Accessibility:** Ensure that digital technology, resources and services are selected and used with accessibility and inclusion in mind. Accessibility features and reasonable adjustments will be used where appropriate to support equitable access for pupils and staff.
- **Use Artificial Intelligence Safely:** Ensure that any generative AI used in school is school-approved, age-appropriate, risk assessed and used in a way that protects safeguarding, privacy, intellectual property and academic integrity. Personal, special-category or confidential information must not be entered into an AI service unless that specific service and use have been formally approved by the school.

3. Teaching and Learning Style

The teaching style for computing at St Agnes is designed to be engaging and interactive. We employ a variety of instructional strategies to accommodate different learning styles, including:

- **Skill Development:** Pupils learn and practice new computing skills directly in the classroom with teacher guidance, ensuring a solid understanding of key concepts.
- **Project-Based Learning:** Encouraging pupils to apply computing skills to real-world problems and projects that interest them.
- **Collaborative Learning:** Facilitating group work where pupils can share their expertise and learn from one another.

Computing Curriculum Planning:

- Our curriculum planning in Computing is rooted in the National Curriculum and further refined by resources from the Department for Education-funded National Centre for

Computing Education (NCCE)**.** In particular, we utilise the lesson planning and curriculum frameworks provided by TeachComputing.org. These resources provide long-term, medium-term, and short-term planning frameworks, which we adapt to fit the specific needs and context of our school.

- Mixed-age classes are managed through a two-year rotational basis to ensure comprehensive curriculum coverage without repetition.

Teaching Computing to Children with Special Educational Needs:

- We provide suitable learning opportunities for all children by setting appropriate challenges and responding to each child's unique needs. Computing has a considerable impact on the quality of work that children produce, increasing their confidence and motivation.
- Where appropriate, pupils will be supported to use accessibility features such as text-to-speech, dictation, captions, zoom and other built-in accessibility tools.

4. Roles and Responsibilities

- **SLT Digital Lead**:
    - **Strategic Oversight:** Develop and maintain the school's digital technology strategy and oversee progress towards meeting all six DfE core digital standards by 2030.
    - **Cyber Security and Safeguarding:** Work with the DSL, DPO and IT support to ensure that digital systems and devices are secure, supported and configured in line with safeguarding, data protection and DfE cyber security expectations.
    - **Digital Governance:** Maintain oversight of device management, approved applications/services, asset and information-asset records, cyber risks, business continuity and the school digital technology strategy. A cyber risk assessment should be completed annually and revisited each term, and significant changes should be addressed promptly.
- **Governing Body:**
    - **Strategic Oversight:** Provide strategic oversight of digital technology, online safety and cyber risk, and approve the Acceptable Use arrangements.
    - **Filtering and Monitoring:** Have overall strategic responsibility for ensuring appropriate filtering and monitoring are in place and seek assurance that the DfE filtering and monitoring standards are being met.
    - **Named Responsibility:** Ensure a named member of SLT and a responsible governor are identified for filtering and monitoring oversight.
- **Headteacher and DSL**:
    - **Oversight:** Ensure this policy aligns with safeguarding, online safety, filtering and monitoring, data protection and behaviour arrangements and is implemented effectively.
    - **Safeguarding:** The DSL leads on safeguarding and online safety, reviews relevant filtering/monitoring alerts and reports, and ensures concerns are acted upon and recorded in line with school safeguarding procedures.

- **Review:** Ensure the policy is reviewed at least annually and following significant changes in technology, working practices, safeguarding risk, BYOD arrangements or the introduction of generative AI products.

- **Computing Coordinator**:
  - **Curriculum Development**: Design and update the computing curriculum to meet educational standards and the needs of our pupils.
  - **Technical Support**: Collaborate with ICT technicians to maintain a secure and effective computing environment.
  - **Professional Development:** Provide training and support for teachers to enhance computing teaching and current online safety knowledge.

- **IT Support / Technical Provider:**
  - Maintain supported, licensed and securely configured systems and devices, apply security updates and maintain anti-malware, firewall, account and access controls.
  - Maintain the technical operation of filtering and monitoring systems, provide reports and carry out actions arising from checks or concerns in collaboration with SLT and the DSL.
  - Enable multi-factor authentication for staff accounts accessing cloud services or remotely accessing on-site systems, and for IT administrative accounts, in line with DfE cyber security standards.
  - Maintain secure backup and recovery arrangements in line with the DfE cyber security core standard and the school's business continuity and disaster recovery arrangements. Support the school's response to and recovery from cyber incidents.

- **Class Teachers**:
  - **Instruction**: Deliver engaging computing lessons that adhere to the curriculum and promote safe technology use.
  - **Monitoring**: Observe pupil activity to ensure compliance with the Acceptable Use Policy and report any issues to the DSL.
  - **Assessment**: Conduct regular assessments of pupil progress and adapt instruction to meet diverse learning needs.

5. Acceptable Use Policy (AUP)

- **General Statement**

  All users must comply with this policy, the relevant Acceptable Use Agreement and other reasonable school instructions. Breaches may result in withdrawal of access, sanctions under the Behaviour Policy, staff disciplinary procedures, suspension or permanent exclusion where applicable, and/or referral to the Headteacher, Governing Body, Local Authority, police or other agencies where required.

- **Use of Computing Equipment**

- **General Conditions:** The 'User' means any pupil, member of staff, governor, volunteer, contractor or visitor using school-owned digital technology, school accounts/services, the school network or an authorised personal device connected to school systems.
- **Equipment Handling:**
  - Users are responsible for the secure and appropriate storage of any computing or ICT equipment taken off school premises. Devices should not be left in cars when unattended.
  - Equipment should be returned regularly if technical work is required.
  - All equipment and devices should be stored securely and not left unattended in insecure locations.
- **Data Protection:**
  - Users must handle personal and confidential data securely and in accordance with UK GDPR, the Data Protection Act 2018, the school Data Protection Policy, privacy notices and any instructions from the DPO.
  - Personal data must not be copied, downloaded, photographed, emailed or transferred outside school-approved systems unless this has been authorised and appropriate security controls are in place.

- **General Conditions for All Users**
  - Users must not:
    - Share passwords, authentication codes or accounts, approve an unexpected multi-factor authentication request, or allow another person to use their login.
    - Install unauthorised software, browser extensions or apps, disable security controls, or use VPNs, proxies, anonymisers or other methods to bypass filtering, monitoring or access restrictions.
    - Open suspicious links or attachments, respond to suspected phishing messages, or continue using an account/device where compromise is suspected; concerns must be reported immediately.
    - Use school systems in a way that infringes copyright, software licences or another person's intellectual property.
    - Change configuration files or settings unless authorised to do so.
    - Use the school's ICT resources to bully, harass, discriminate against, threaten or otherwise cause harm to another person, or violate their privacy.
    - Access, store, transfer, or display illegal, offensive, or inappropriate materials, including but not limited to pornography, hate sites, or violent content.
    - Engage in gaming, gambling, or personal profit activities using school ICT equipment unless it is part of a sanctioned educational activity.

        - Violate or attempt to violate any computer network's system security, including accessing unauthorised systems.

- **Computer Access Agreement**
    - **Staff and Pupils:**
        - Access to computing or ICT equipment is granted for educational purposes, including research, teaching, and administrative tasks related to school functions.
    - **Visitors:**
        - Visitors may be granted access to the school Guest Wi-Fi where appropriate. Guest access must be separated from the main school network, remain subject to appropriate filtering, and be used only for lawful purposes connected with the visit.

- **Use of Social Media and Mobile Phones**
    - **Social Media:**
        - The use of social media on school devices is only permitted if the school has its own official accounts, and usage aligns with school policies.
    - **Mobile Phones:**
        - In line with statutory guidance applying from 1 September 2026, pupils must not use or access mobile phones during the school day. This expectation also applies to smartwatches and other communication-enabled personal devices covered by the school rules. Any device brought to school must be switched off and stored in accordance with school procedures. Unauthorised use may result in confiscation in line with the Behaviour Policy. Individual exceptions may be agreed where required for medical, SEND, safeguarding or other reasonable-adjustment reasons.
        - Staff must not use personal phones or other personal devices to photograph, film or make audio recordings of pupils unless the Headteacher has expressly authorised a specific exceptional use and an approved method of secure transfer/deletion has been agreed. School-owned devices should be used wherever possible.
- **Data Protection and Security:**
    - **Data Security:**
        - Data should be handled according to the school's Data Protection Policy, ensuring that it is processed securely and in compliance with relevant regulations.
        - Use of personal devices (BYOD) to access school systems or data is permitted only where explicitly authorised by the school and where the device and method of access meet the controls below.

- **Bring Your Own Device (BYOD) and Personal Devices**
    - The school does not accept responsibility for ordinary loss of, or damage to, personal devices brought onto the premises except where liability arises in law. Users remain responsible for the physical security and lawful use of their personal devices.
    - Personal laptops, tablets, phones, smartwatches and other connected devices must not access school data or systems unless the school has authorised that use.
    - Authorised personal devices must use a supported operating system, current security updates, a screen lock/PIN or biometric lock and appropriate device encryption where available. Staff must use multi-factor authentication where required by the school.
    - School data must not be stored in personal photo galleries, personal email accounts, consumer cloud backups or shared/family accounts. Local downloads should be avoided unless specifically authorised.
    - Loss, theft, malware, suspicious access or compromise of a device used for school work must be reported immediately to the SLT Digital Lead/IT support and, where personal data may be involved, the DPO.
    - Authorised personal devices used under the school's BYOD arrangements may connect to the designated school network and are subject to the school's filtering, monitoring and security controls. Personal hotspots, tethering, mobile data, VPNs or proxy services must not be used to provide pupils or school devices with unfiltered internet access or to circumvent school controls.
    - The school may restrict, withdraw or refuse BYOD access where a device cannot be adequately secured, filtered or managed, or where use creates a safeguarding, data protection or cyber-security risk.
- **School Policy Principles**
    - **ICT Devices for Official Use:**
        - ICT devices are provided solely for official and approved purposes, not for personal gain or running a private business.
        - Limited and reasonable personal use of school ICT devices is permissible, provided it does not interfere with school operations and complies with this policy.
        - Users must lock devices or sign out when leaving them unattended and must not leave sensitive information visible to others.
        - Only school-approved software, applications, cloud services and AI tools may be used for school business or pupil learning where personal data, safeguarding information or school systems are involved.

- **Health & Safety**
    - **Electrical Safety:**
        - Electrical equipment must be maintained so that it remains safe. User checks, formal visual inspection and, where appropriate, electrical testing/PAT will be carried out at intervals determined by risk, equipment type, environment, manufacturer advice and previous inspection results. Annual PAT testing of every portable item is not a legal requirement. Personal mains-powered electrical equipment may only be used with prior school approval and may be subject to inspection or testing before use.
        - Personal or unencrypted USB storage and other removable media must not be used on school systems. Where removable media is operationally necessary, it must be school-authorised, appropriately encrypted where it contains personal/confidential data, and handled in accordance with IT support instructions.
        - Pupils must not connect, disconnect or handle mains electrical equipment unless this is specifically permitted and appropriately supervised. Damaged cables, plugs, chargers or equipment must be taken out of use and reported immediately.

6. Incident Reporting and Response

- **Safeguarding Incidents:** Staff must report online-safety or safeguarding concerns to the DSL without delay using CPOMS and follow the school Safeguarding/Child Protection Policy.
- **Cyber / Technical Incidents:** Suspected phishing, malware, compromised accounts, unauthorised access, loss/theft of devices or other cyber incidents must be reported immediately to IT support and the SLT Digital Lead. Users should not delete evidence or attempt their own technical investigation.
- **Data Breaches and Records:** Where personal data may have been compromised, the DPO must be informed promptly. Safeguarding, cyber and data incidents must be recorded with actions and outcomes in the appropriate school system.

7. Training and Professional Development

Ongoing training is essential for maintaining a high standard of computing education:

- **Staff Training:** Regular and up-to-date training on computing, online safety, safeguarding, phishing/social engineering, password and MFA security, personal data breaches, safe use of AI and the risks of removable media and BYOD.
- **Pupil Education:** Age-appropriate teaching on digital literacy, online safety, cyber security, privacy, reliable information, responsible AI use and how to report anything that worries them.

- **Parent Engagement:** Information and resources to help parents reinforce online safety, mobile-phone expectations, digital resilience and responsible technology use at home.

8. Health and Safety

- Electrical equipment will be maintained under a risk-based inspection and testing regime. Staff should not bring personal mains-powered electrical equipment into school unless it is necessary and has been approved. Any required inspection or testing will be determined by the school's competent person/risk assessment rather than by an automatic annual PAT rule.
- Unauthorised or unencrypted removable media is prohibited. School-authorised removable media may be used only where required and subject to security controls. Damaged or unsafe equipment must be reported and taken out of use immediately.
- Specific guidelines for the safe use of iPads, laptops, and other devices, including transportation and storage protocols, should be followed rigorously.

9. Resources

- Laptops/Chromebooks
- iPads
- Network Printer (School Office)
- Network Scanner (School Office)
- Digital cameras
- Beebots / Roamers
- Control interface with buzzers etc.
- Interactive televisions, whiteboards & projectors
- Handheld learning devices e.g. microbits

10. Monitoring and Review

- **Policy Evaluation:** Review this policy at least annually against safeguarding, curriculum, data protection, cyber-security and DfE digital and technology requirements.
- **Filtering and Monitoring Link:** The school will review filtering and monitoring at least once each academic year and following significant changes such as BYOD/remote-access changes, new devices, generative AI tools or major network/software changes. Results and actions are recorded under the separate Filtering and Monitoring Policy.
- **Continuous Improvement:** Amend the policy where changes in technology, incidents, school practice or risk indicate that controls, curriculum or training need to change.

11. Data Protection, Privacy and Artificial Intelligence

- **General Data Handling**:

- Personal data arising from computing and ICT use will be processed in accordance with UK GDPR, the Data Protection Act 2018, the school Data Protection Policy, retention arrangements and relevant privacy notices.
- Access to personal data, device/network logs and safeguarding information will be limited to authorised personnel who require it for their role. Monitoring arrangements must be transparent and reflected in relevant privacy information; DPIAs will be completed where high-risk processing requires one.

- **Use of AI Tools**:
  - **All use of artificial intelligence for school purposes must also comply with the school's Artificial Intelligence Policy.**
  - **Approved AI Use:** Staff and pupils must use only AI products and features approved by the school for the intended age group and purpose. Personal, special-category, safeguarding or confidential information must not be entered into an AI service unless the school has specifically approved the product and processing, including the necessary data-protection and contractual safeguards.
  - **Safe Practice:** Users must check AI outputs for accuracy, bias and suitability; must not use AI to create harmful, deceptive, sexualised or abusive content (including deepfakes); and must follow school expectations on copyright and academic integrity. Pupil-facing use must be appropriately supervised and comply with provider age restrictions.
  - **Risk Review:** New or materially changed AI tools must be considered through the school's approval/risk-assessment process, including safeguarding, filtering/monitoring, privacy and cyber-security implications. The school will take account of the DfE Generative AI Product Safety Standards when assessing products.

12. Key References

- Keeping Children Safe in Education 2026 (effective 1 September 2026).
- DfE Meeting digital and technology standards in schools and colleges, including the Filtering and Monitoring and Cyber Security core standards (updated August 2026).
- DfE Mobile phones in schools statutory guidance (to be followed from 1 September 2026).
- DfE Generative AI: product safety standards (2026).
- UKCIS Education for a Connected World framework.
- School Online Safety, Artificial Intelligence, Filtering and Monitoring, Data Protection, Safeguarding/Child Protection and Behaviour policies.

13. **Protecting Personal Data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR).

- The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy.

- All data will be handled in accordance with the school's Data Protection Policy.

Data Audit For This Policy					
What ?	**Probable Content**	**Why ?**	**Who ?**	**Where ?**	**When ?**
User accounts	Name, username, email address, role/access permissions	Authentication, access and administration	Authorised SLT / IT support	Approved school/cloud systems	For account life plus applicable retention period
Device / network logs	Device identifiers, login and access logs	Cyber security, troubleshooting and audit	IT support / authorised SLT	School network and approved cloud systems	In line with the school retention schedule and provider settings
Filtering / monitoring data	Web activity, alerts and monitoring reports	Safeguarding and online safety	DSL / authorised SLT / IT support	Approved filtering and monitoring systems	In line with the Filtering and Monitoring Policy and relevant privacy information
Device assignment / support	Asset number, assigned user and repair/support records	Asset management, security and technical support	Authorised school staff / IT support	Asset register / approved support systems	In line with the school retention schedule

- As such, our assessment is that this policy :

Has Few / No Data Compliance Requirements	**Has A Moderate Level of Data Compliance Requirements**	**Has a High Level Of Data Compliance Requirements**
		✓